Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 57 (2015) 752 – 756

Procedia Computer Science

3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)

# Securing Voice Call Transmission over Cellular Communication

Daya Sagar Gupta[a], G. P. Biswas[b], a*

*Department of Computer Science and Engineering, Indian School of Mines, Dhanbad-826004, Jharkhand, India*

**Abstract**

Voice call transmissions on cellular networks are not end-to-end secure and thus, attacks like call tracing, modification etc by an adversary is easily feasible, that is, any adversary Eve, can trace the call, and can intercept the voice, which is transmitted over an unsecured medium from a user (Alice) to another user (Bob) through mobile phones. Thus, it's not safe to private talk on the mobile phones. In this paper, we propose a scheme, which provides entire security between valid end users over the security protection provided by the network system. A common secret key is pre-negotiated between end users (many such schemes are available) to initiate the communication. We present a global construction of our proposed protocol. In addition to this, we also discuss the security proofs of our proposed protocol.


Peer-review under responsibility of organizing committee of the 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)

*Keywords:* Key generation; hash function; cellular communication; linear-feedback shift register

## 1. Introduction

Secure mobile voice communication is an open problem in the field of mobile network security. In recent years, several different types of protocols are proposed in the direction of this problem. In year 2004, Katugampala, Al-Naimi, Villette and Kondoz [2] proposed a scheme in which they described a real time prototype implementation of a system, which enables secure voice and data communication over the GSM

* Daya Sagar Gupta. Tel.: +91-9709202933
*E-mail address:*dayasagar.ism@gmail.com.


Peer-review under responsibility of organizing committee of the 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015)
doi:10.1016/j.procs.2015.07.469

voice channel. In year 2005, they [3] proposed a modified version of [2] in which a real-time prototype is implemented demonstrating the end-to-end secure voice communications over the GSM voice channel. In year 2007, Chia-Hui Wang and Mei-Wen Li [11] proposed that a distributed multi-key solution which dynamically changes the encryption key based on the Diffie-Hellman algorithm to provide more secure protection for an end-to-end VoIP call. In this paper, we propose a quiet simple technique for securing the mobile communication using the pre-negotiated common key between end users. We also use the concepts of linear-feedback shift register (LFSR) [8, 9] in primitive polynomial to implement our protocol. We have also shown that our proposed protocol is secure against possible attacks.

The rest of the paper is organized as follows: Section 2 describes some background ideas about key-negotiation techniques and LFSR. In section 3, the proposed scheme is presented. The security analyses of our scheme are described in section 4, and we conclude the paper in section 5.

## 2. Preliminaries

In this section, we first introduce about key generation techniques and then we give some background on LFSR with primitive polynomial.

### *2.1 Key-Negotiation Protocols*

The first proposed key generation protocol is Diffie-Hellman (DH) protocol [1].This protocol allows two users to exchange a common secret key between them over an insecure medium described as follows: Suppose two users, Alice and Bob willing to exchange a common key for secure communication. Both agree upon two numbers $g$ and $q$, where $q$ is a prime and $g$ is a generator of order $q$ in the group $<Z_{q^*}, *>$.The steps are follows:

a. Alice chooses a large random number $x_a<q$ and calculates $u = g^{x_a} \ mod \ q$ and sends $u$ to Bob.
b. Similarly, Bob chooses another large random number $x_b<q$ and calculates $v = g^{x_b} \ mod \ q$ and sends $v$ to Alice.
c. Alice calculates $K = v^{x_a} mod q$.
d. Bob calculates $K = u^{x_b} mod \ q$.

Now both Alice and Bob have the same secret key, namely $K = g^{x_a x_b}$. However, this protocol suffers some attacks like man-in-the-middle (MITM) attack etc. Many other key-generation protocols are proposed in account to better security [4, 5, 8, 9, 10 etc].

### *2.2 Linear-feedback shift register*

Linear feedback shift registers (LFSR) is a circuit used to generate pseudorandom number [8, 9]. The LFSR can be created by using a chain of flip-flops. The linear-feedback shift register is a mechanism for generating a sequence of binary bits. The register initialized by the vector secret seed. The behaviour of the register is regulated by a clock and the XOR of a subset of the bit contents is placed in the rightmost bit. The LFSR can hold the longest period when the polynomial of tap sequence adding 1 is primitive polynomial. To obtain the longest period of (2n*)* −1, LFSR with length $n$ need to find $n$ exponent primitive polynomial in GF (2). From the security of cryptography, the longer period is the better option. Leftmost bit is used as a bit of key stream and is next input bit.

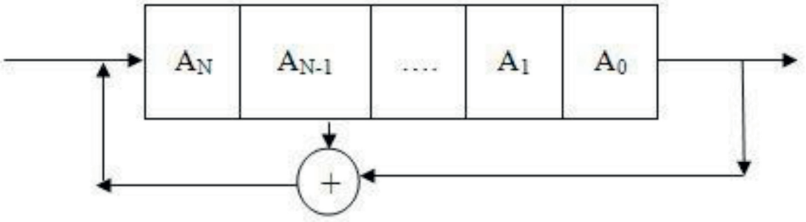


Fig. 1. Linear-feedback shift register

## 3. Proposed Scheme

This section presents an efficient security schemes, which describes the way, by which the users of mobile communication ensure that their voice does not tapped *i.e.* their communication is secure. To describe our proposed protocol, we consider that a common secret key $\kappa$ is negotiated between the end users, Alice and Bob using a secure and efficient key exchange protocols [1, 4, 5, 8, 9, 10 etc]. Further, they both are agreeing on a common pre-negotiated LFSR and a hash function $h$ to implement the proposed scheme. The steps of proposed protocol are described as follows:

*Step 1:* Alice chooses a random integer $i$ and compute the hash of secret key $\kappa$, $i$ times, using the hash function $h$ *i.e.* $h(\kappa) = x_1$, $h(x_1) = x_2$ ..... $h(x_{i-1}) = x_i$ and set the bits of $x_{i-1}$ in vector seed of LFSR.

*Step 2:* Alice's voice (analog data) is then converted into digital data through an ATD converter as in fig. 2 and then, is XORed with the output of LFSR, say $x$. The XORed data, say $C = m \oplus x$ is then goes to the Bob with concatenation of $x_i$ *i.e.* $C \| x_i$.

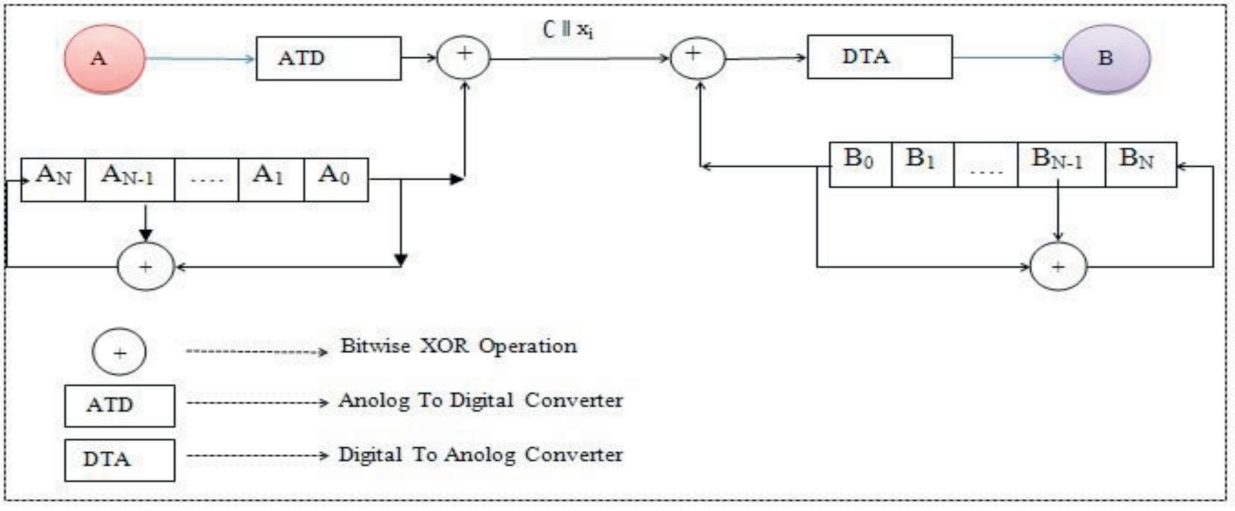


Fig.2.Design of secure voice call transmission

*Step 3:* At the other end, Bob computes repeated hash of common secret key $\kappa$ continuously and count the number of iteration at which, it is equal to the incoming $x_i$ from Alice and sets the output of *i-1* iteration of hash into the seed of same LFSR as Alice. So, the content of both LFSRs will be same.

*Step 4:* The incoming digital message $C$ from Alice is, then XORed with the output of the Bob's LFSR and passes through a DTA converter. Thus, Bob gets the original secure voice coming from Alice.

As a proof of verification, the receiver end computation is $m \oplus x \oplus x = m$ thus original message is decrypted by Bob.

However, the proposed protocol uses a pre-negotiated LFSR between the end users and there are several pairs of such mobile users who want to communicate securely in the universe. Thus, one common LFSR must be used and known to every mobile user for each communication globally which is difficult to implement. To resolve this difficult, here we gave a practical construction about LFSR as shown in fig.3. Every mobile user has the contact number of her friend in her friend list to call him. Likewise contact number; she also must know the LFSRs of each friend with their contact number to construct our proposed scheme *i.e.* if a mobile user *U* has *n* friends namely, $F_1$, $F_2$..... $F_n$, then user *U* must know about their LFSRs, say, $LFSR_1$, $LFSR_2$..... $LFSR_n$. Whenever she wishes to communicate, she must know the contact number as well as LFSR of other party. In this manner, we use different types of LFSRs in each pair of communication to avoid a single LFSR globally as fig.3.

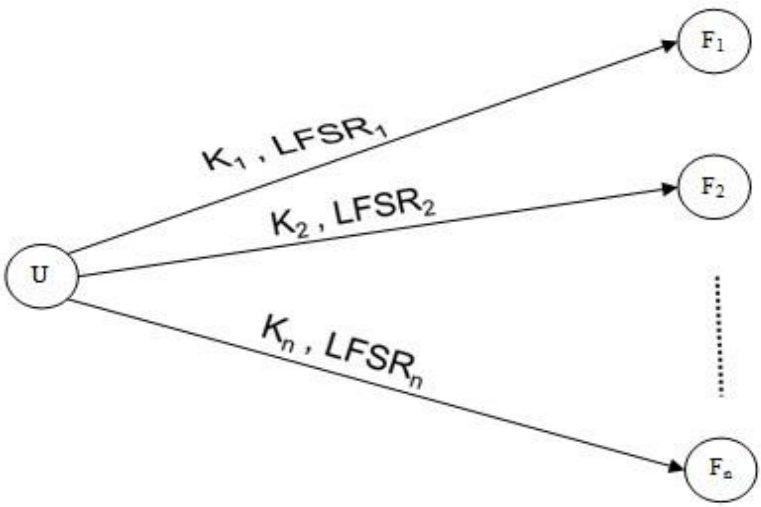


fig.3. Stucture of proposed protocol

## 4. Security Analyses

This sub-section addresses the security analysis of our proposed schemes. The protocol is well protected against call tracing. Talking about security to our proposed schemes, let an adversary, say, Eve intercepts the message in between the communication. Obviously, she gets $C \| x_i$ which is transmitted during the communication but she is unable to intercept the original data *m* because she do not know the common secret key $\kappa$. Suppose, Eve tries to find the content of LFSR using the pattern of data in between the communication for a long time, she will be unable to guess because the output of LFSR is not constant and always changes from *x* to *x'*. Since both, message and output of LFSR is changed repeatedly, the Eve is unable to find any meaningful information. Now, if Eve tries to find $x_{i-1}$ using $x_i$, she will be unable because hash function is a one-way function and reverse of hash is not possible.

## 5. Conclusions

In this paper, we have proposed a mobile communication scheme which avoids the tracing of voice calls on the mobiles networks. The proposed protocol is based on the hardness of LFSR and hash function. The key generation techniques in this protocol play an important role to secure the communication. We also showed that our protocol is secured under voice call tracing and modification.

## References

[1] W. Diffie and M. E. Hellman “New Directions in Cryptography", *IEEE Trans. Info. Theory*, vol. 22, pp.644 -654 1976

[2] N. N. Katugampala , K. T. Al-Naimi , S. Villette and A. M. Kondoz "Real time data transmission over GSM voice channel for secure Voice and data applications", *Proc. 2nd IEE Secure Mobile Commun. Forum: Exploring Tech. Challenges Secure GSM WLAN (Ref. No. 2004/10660)*, pp.7/1 -7/4 2004

[3] N. N. Katugampala, K. T. Al-Naimi, S. Villette, and A. M. Kondoz, "Real-time End-to-end Secure Voice Communications over GSM Voice Channel," 13th European Signal Processing Conference (EUSIPCO'05), Turkey, Sep. 2005.

[4] A. Joux and K. Nguyen. Separating Decision Diffie-Hellman from Diffie-Hellman in Cryptographic Groups. Cryptology ePrint Archive, Report-2002/03.

[5] H. Krawczyk "SKEME: A Versatile Secure Key Exchange Mechanism for Internet", *Proc. Internet Soc. Symp. Network and Dist. Sys. Security*, 1996

[6] http://school.maths.uwa.edu.au/~praeger/teaching/3CC/WWW/chapter4.html

[7] Haraf M, Mansour H A K, Zayed H. A Complex Linear Feedback Shift Register Design for the A5 Key streamGenerator [C/OL].[2006-04-20]

[8] Tsudik, G., Steiner, M., Waidner, M.: Diffie-Hellman key distribution extended to groups. In: Proceedings 1996 ACM Conference on Computer and Communications Security (1996)

[9] Y. Hitchcock, C. Boyd, J.M.G. Nieto. Tripartite key exchange in theCanetti-Krawczyk proof model. In: INDOCRYPT 2004, in: LNCS, vol.3348. Springer-Verlag, 2004, pp.17-32.

[10] Lee, B., Boyd, C., Dawson, E., Kim, K., Yang, J., Yoo, S.: Secure key issuing in id-based cryptography. In: Hogan, J.M., Montague, P., Purvis, M.K., Steketee, C. (eds.) ACSW Frontiers. CRPIT, vol. 32, pp. 69–74. Australian Computer Society (2004)

[11] Chia-Hui Wang, Mei-Wen Li "A Distributed Key Changing Mechanism for Secure Voice-Over-IP Service", 2007 IEEE International Conference on Multimedia and Expo, 2007